BAB I
PENDAHULUAN

I.1 Latar Belakang

Sejak mulainya era digital di abad ke-20, semakin banyak orang yang menyimpan datanya secara elektronik. Fenomena ini tidak hanya menjadi tren di kalangan individu atau perseorangan, tetapi juga di antara hampir semua bisnis yang mengandalkan kenyamanan arsip digital untuk menyimpan data mereka secara terkomputerisasi atau disimpan secara digital. Namun, muncul pula bentuk kejahat baru yakni peretasan data-data oleh individu yang tidak bertanggung jawab yang berusaha melakukan kejahatan dengan informasi pribadi yang mereka peroleh. Tidak hanya itu, salah satu bahaya dari data digital juga adalah penyalahgunaan data tersebut oleh pihak-pihak yang justru dipercayai untuk menyimpan informasi tersebut. Tindakan peretasan data pribadi atau penyalahgunaan data pribadi oleh perusahaan ini dapat dikategorikan sebagai kejahatan dunia maya atau disebut *cybercrime*.

Secara umum, definisi *Cybercrime* adalah "kegiatan kriminal yang dilakukan dengan menggunakan komputer atau Internet."[1] Kejahatan dunia maya telah berkembang pesat dengan kemajuan teknologi yang dibuat manusia. Dengan segala upaya yang dilakukan untuk menutup pintu pembobolan data oleh pihak ketiga, sepertinya para pelaku kejahatan juga telah melangkah lebih jauh dalam menyempurnakan kejahatannya. Upaya untuk menjauhkan penjahat dunia maya ini pada dasarnya hanyalah langkah preventif untuk mengurangi kemungkinan pelanggaran data dapat terjadi pada setiap individu. Akan tetapi cara terkuat untuk membatasi penjahat dunia maya ini adalah dengan memberlakukan undang-undang terkait perlindungan data pribadi dan menjatuhkan hukuman, baik itu sanksi administratif atau hukuman pidana untuk kejahatan mereka.

[1] https://pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/ /#:~:text=Cybercrime%20is%20defined%20as%20a,information%2C%20or%20disable%20a%20device., diakses pada tanggal 26 Oktober 2020

Undang-undang perlindungan data dan privasi masih dapat dianggap sebagai topik yang relatif masih baru muncul di dunia hukum, karena belum banyak negara yang telah menerapkan undang-undang perlindungan data dan privasi. Menurut Dewan Teknologi Forbes (*Forbes Technology Council)*, *data privacy* adalah tentang menjaga informasi anda agar tidak dijual atau dibagikan, sementara *data protection* berfokus pada menjaga informasi itu dari peretas.[2] Tidak banyak negara yang memiliki undang-undang yang pasti dan kokoh terkait perlindungan data dan privasi. Salah satu undang-undang paling lengkap dan terbaru terkait perlindungan data dan privasi adalah *General Data Protection Regulation* (selanjutnya disebut GDPR) oleh Uni Eropa yang diundangkan pada tanggal 25 Mei 2018. GDPR menjadi model bagi banyak undang-undang nasional oleh negara non-Uni Eropa termasuk Indonesia karena merupakan salah satu sumber hukum terkini mengenai perlindungan data pribadi. Mengenai undang-undang tersebut, Indonesia sendiri masih kekurangan departemen ini, di mana saat ini tidak ada undang-undang definitif atau spesifik yang ditulis untuk menangani kejahatan perlindungan data pribadi dan tanggung jawab perusahaan untuk melindungi privasi data pelanggan mereka.

Undang-undang terkait yang ada tentang privasi data terbatas pada perlindungan data keuangan, kesehatan, dan komunikasi saja. Peraturan mengenai perlindungan data pribadi di Indonesia belum terkodifikasi dalam satu undang-undang yang khusus, melainkan tersebar dalam berbagai peraturan perundang-undangan lainnya. Namun, data pribadi telah diatur sedikit dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) dalam Pasal 26 ayat (1) yang menyatakan:

> "Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

[2] https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#42f7ad350c9e, diakses pada tanggal 26 Oktober 2020

Pasal tersebut tidak menjelaskan definisi dari data pribadi, oleh sebab itu dalam penjelasan Pasal 26 ayat (1) UU ITE dinyatakan:

> "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:
> a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
> b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
> c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

UU ITE tidak menyebutkan definisi dari data pribadi itu sendiri diluar dari penjelasan yang ada bagi Pasal 26 tersebut diatas. Oleh sebab itu, untuk mengisi kekosongan hukum terkait dengan perlindungan data pribadi dikeluarkanlah Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi (selanjutnya disebut Permenkominfo Perlindungan Data Pribadi.) Perkominfo Perlindungan Data Pribadi memberikan definisi konkret bagi data pribadi yakni dalam Pasal 1 angka 1 yang menyatakan "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannya".

Menurut UU ITE, tanda tangan elektronik wajib diamankan. Hal tersebut diatur dalam pasal 12 UU ITE yang menentukan:

1. "Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya.
2. Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang- kurangnya meliputi:
    a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak;
    b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;
    c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:
        1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau

2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

3. Setiap Orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul."

Terkait dengan penyimpanan data pribadi sendiri dilakukan oleh Penyelenggara Sistem Elektronik yang dalam Pasal 1 angka 6a adalah:

> "Setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain."

Walau tidak disebutkan secara langsung, telah diatur oleh UU ITE bagi perilaku Penyelenggara Sistem Elektronik terhadap informasi yang dikelolanya, dan ini tentunya termasuk data pribadi, sesuai dengan ketentuan Pasal 15 yang menyatakan:

1. "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
2. Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
3. Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik."

Yang kemudian persyaratan bagi kinerja Penyelenggara Sistem Elektronik sesuai dengan Pasal 16 adalah:

1. "Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:
    1. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
    2. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

3. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
4. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
5. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

2. Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah."

Pada tahun 2015 Indonesia mulai membahas Rancangan Undang-Undang (selantjutnya disebut RUU) Perlindungan Data Pribadi, namun karena pembahasan yang macet, hingga saat ini RUU tersebut tidak disahkan. Untuk meletakkan landasan sambil menunggu undang-undang yang lebih tinggi dan komprehensif disahkan, pada tahun 2016 Kementerian Komunikasi dan Informatika mengesahkan Permenkominfo Perlindungan Data Pribadi. Namun, peraturan ini tidak secara jelas mendefinisikan hak pemilik data dan kewajiban pengontrol dan pemroses data. Peraturan ini juga tidak menerapkan sanksi pidana, melainkan pelanggar hanya akan mendapatkan sanksi administratif seperti, pembekuan izin. Memasuki tahun 2020, dengan hal ini Kementerian Komunikasi dan Informatika masih terus berjuang untuk mendorong RUU ini ke DPR agar segera disahkan karena sudah masuk dalam Program Legislatif Nasional (PROLEGNAS). Akibat dari belum disahkannya RUU Perlindungan Data Pribadi, banyak kasus-kasus pencurian data yang penyelesaiannya masih tidak bisa didasarkan hukum yang lebih spesifik terkait data pribadi.

Salah satu kasus besar yang terjadi pada tahun 2020 adalah peretasan data 91 juta pengguna aplikasi *e-commerce* yaitu Tokopedia. Diketahui ada pihak-pihak peretas atau disebut *hacker* yang berhasil mencuri data pengguna aplikasi Tokopedia dan kemudian menjual data tersebut di *dark web*. *dark web* sendiri merupakan "bagian dari internet yang tidak tercantum dalam mesin pencari"[3] dan umumnya digunakan untuk melakukan transaksi-transaksi yang illegal. Kasus bocornya data pribadi pengguna akun Tokopedia ini sendiri diungkap oleh

[3] https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html, diakses pada tanggal 26 Oktober 2020

seseorang melalui Twitter yaitu pengguna akun @underthebreach yang mengklaim bahwa ia adalah seorang petugas layanan pengawasan dan pencegahan kebocoran data dari Israel.[4] Terungkap bahwa ada seorang *hacker* yang berhasil meretas data-data pengguna Tokopedia pada 20 Maret 2020 dan menjual data tersebut yang berupa "User Id, email, nama lengkap, tanggal lahir, jenis kelamin, nomor ponsel dan password tersandi"[5] kepada pembelinya. Pihak Tokopedia sendiri juga telah mengkonfirmasi adanya kebocoran data pengguna mereka, namun pihak Tokopedia menyatakan bahwa data yang diambil tidak membahayakan saldo pengguna karena adanya keamanan berlapis, sehingga data terkait perbankan pengguna tidak terambil oleh *hacker*. Kasus ini pun telah dilaporkan oleh pihak Tokopedia kepada pemerintah dan terutama pada Kementerian Komunikasi dan Informatika terkait penyelesaian kasus ini, tetapi belum ada tindakan hukum secara langsung bagi terjadinya pencurian data. Pihak Tokopedia hanya menghimbau para penggunanya untuk mengganti sandi mereka agar mencegah data-data mereka untuk mudah diretas apabila data tersebut termasuk data yang telah dicuri dalam peretasan 20 Maret 2020.

Kelanjutan dari kasus peretasan Tokopedia ini tidak ditindaklanjuti secara hukum, dikarenakan belum disahkannya Undang-Undang tentang Perlindungan Data Pribadi. Namun, hal ini tentunya tidak bisa dibiarkan terjadi begitu saja karena pasti menimbulkan kerugian dari pihak pengguna yang datanya telah diretas oleh pihak-pihak ketiga yakni, *hacker*. Atas dasar pemaparan latar belakang diatas, penulis tertarik menulis tesis dengan judul "**Analisis Yuridis Pertanggungjawaban Perusahaan dan Pelaku Saat Terjadinya Pencurian Data Pribadi Pengguna Aplikasi Tokopedia"**

I.2 Rumusan Masalah

Atas dasar latar belakang tersebut di atas penulis memberikan rumusan masalah sebagai berikut:

[4] https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia, diakses pada tanggal 26 Oktober 2020

[5] *Loc.cit*

1. Siapakah yang bertanggung jawab atas pencurian data pribadi pengguna aplikasi Tokopedia?
2. Apakah bentuk sanksi yang bisa dijatuhkan kepada perusahaan sebagai penyimpan data pribadi ketika terjadi *security breach?*

I.3 Tujuan Penulisan

A. Tujuan Akademis

a. Untuk memenuhi salah satu syarat akademis guna memperoleh gelar Magister Hukum (M.H) di Fakultas Hukum Universitas Pelita Harapan Kampus Surabaya

b. Untuk memberikan sumbangan bagi ilmu pengetahuan khususnya dalam bidang hukum Perlindungan Data Pribadi

c. Dapat memberikan atau menambah perbendaharaan pustaka terutama dalam bidang hukum Perlindungan Data Pribadi

B. Tujuan Praktis

a. Untuk lebih memahami tentang akibat hukum pelaku pencurian data pribadi menurut peraturan perundang-undangan di Indonesia.

b. Untuk lebih memahami bentuk pertanggung jawaban atau pun sanksi bagi perusahaan yang telah mengalami *security breach* sebagai penyimpan data pribadi pengguna.

c. Untuk lebih meningkatkan wawasan tentang aturan-aturan mengenai perlindungan data pribadi di Indonesia.

I.4 Metode Penelitian

Penelitian adalah suatu sarana pokok dalam pengembangan ilmu pengetahuan maupun teknologi yang bertujuan untuk mengungkapkan kebenaran secara sistematis, metodologis dan konsisten.[6]

A. Tipe Penelitian

Tipe penelitian yang digunakan dalam penyusunan tugas akhir ini adalah tipe penelitian yuridis normatif. “Penelitian hukum normatif yang nama lainnya adalah penelitian hukum doktrinal yang disebut juga sebagai

[6] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif,* Raja Grafindo Persada, Jakarta, 2014, h.1

penelitian perpustakaan atau studi dokumen karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum yang lain"[7].

B. Pendekatan Masalah

Pendekatan yang digunakan dalampenelitian ini adalah pendekatan perundang-undangan dan pendekatan konseptual. Menurut Peter Mahmud Marzuki, pendekatan perundang-undangan adalah "Pendekatan undang-undang dilakukan dengan menelaah semua undang undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani." [8] Pendekatan Konseptual adalah: "beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum. dengan mempelajari pandang-pandangan dan doktrin-doktrin di dalam ilmu hukum, peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum, konsep-konsep hukum, dan asas-asas hukum relevan dengan isu yang dihadapi. Pemahaman akan pandangan-pandangan dan doktrin-doktrin tersebut merupakan sandaran bagi peneliti dalam membangun suatu argumentasi hukum dalam memecahkan isu yang dihadapi."[9]

C. Bahan Hukum

1. Bahan hukum primer adalah bahan hukum yang mempunyai otoritas. Bahan hukum primer yang digunakan dalam penelitian ini adalah

   a) General Data Protection Regulation

   b) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   c) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

   d) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi

---

[7] *Ibid* h. 14.
[8] Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana, Jakarta, 2006, h. 93.
[9] *Ibid,* h.95.

e) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
f) Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdangan Melalui Sistem Elektronik
g) Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

2. Bahan Hukum Sekunder adalah bahan hukum yang menunjang bahan hukum primer, tidak bersifat mengikat tetapi menjelaskan mengenai olahan pendapat atau doktrin para ahli. Bahan hukum sekunder meliputi:
   a) Buku/literatur yang terkait permasalahan yang akan diteliti
   b) Artikel-artikel
   c) Yurisprudensi
   d) Rancangan Undang-Undang Perlindungan Data Pribadi

D. Langkah Penelitian

a. Langkah Pengumpulan Bahan Hukum

Penulis memulai mengumpulkan bahan hukum dengan menggunakan cara inventarisasi, kualifikasi dan sistematisasi. Inventarisasi adalah pengumpulan bahan hukum yang dilakukan melalui studi pustaka yang terkait dengan isu hukum yang dikemukakan. Kualifikasi adalah memilah-milah bahan hukum yang diperoleh melalui inventarisasi yang disesuaikan dengan bahan hukum untuk menjawabnya. terakhir, sistematisasi adalah penyusunan bahan hukum menjadi sedemikian rupa untuk lebih mudah membaca dan memahaminya.

b. Langkah Analisa

Sebagai tipe penelitian yuridis normatif, metode yang digunakan adalah "metode deduksi" yaitu dimulai dari ketentuan atau hal-hal yang bersifat umum dalam hal ini adalah perjanjian internasional, asas-asas internasional, doktrin, serta teori-teori yang ditemukan dalam literatur yang diterapkan pada rumusan masalah untuk menghasilkan jawaban yang bersifat khusus. Untuk lebih memperoleh jawaban yang sahih digunakan penafsiran otentik dan sistematis. Penafsiran otentik adalah penafsiran

berdasarkan definisi yang sudah ada di peraturan perundang-undangan. Penafsiran Sistematis adalah penafsiran dengan cara menghubungkan pasal-pasal yang ada dalam satu peraturan perundang-undangan sama atau dalam peraturan perundang-undangan yang berbeda.

I.5 Kerangka Teoritik

Permenkominfo Perlindungan Data Pribadi dalam Pasal 1 angka 1 menyatakan "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannya." Pasal 1 Angka 2 menentukan bahwa:

> "Data Perseorangan Tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan."

Pasal 1 angka 5 Permenkominfo Perlindungan Data Pribadi menyatakan bahwa:

> "Sistem Elektronik adalah serangkaian perangkan dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik."

Sedangkan Penyelenggara Sistem Elektronik menurut Pasal 1 angka 6 Permenkominfo Perlindungan Data Pribadi adalah:

> "Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain."

Dalam Pasal 2 Permenkominfo Perlindungan Data Pribadi diatur mengenai Perlindungan Data Pribadi Dalam Sistem Elektronik yang ketentuannya adalah sebagai berikut:

1. "Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi.

2. Dalam melaksanakan ketentuan sebagaimana dimaksud pada ayat (1) harus berdasarkan asas perlindungan Data Pribadi yang baik, yang meliputi:
   a. penghormatan terhadap Data Pribadi sebagai privasi;
   b. Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan;
   c. berdasarkan Persetujuan;
   d. relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
   e. kelaikan Sistem Elektronik yang digunakan;
   f. iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi;
   g. ketersediaan aturan internal pengelolaan perlindungan Data Pribadi;
   h. tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna;
   i. kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi; dan
   j. keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.
3. Privasi sebagaimana dimaksud pada ayat (2) huruf a merupakan kebebasan Pemilik Data Pribadi untuk menyatakan rahasia atau tidak menyatakan rahasia Data Pribadinya, kecuali ditentukan lain sesuai dengan ketentuan peraturan perundang-undangan.
4. Persetujuan sebagaimana dimaksud pada ayat (2) huruf b diberikan setelah Pemilik Data Pribadi menyatakan konfirmasi terhadap kebenaran, status kerahasiaan dan tujuan pengelolaan Data Pribadi.
5. Keabsahan sebagaimana dimaksud pada ayat (2) huruf j merupakan legalitas dalam perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi."

Selanjutnya, definisi data pribadi diatur pula menurut Pasal 1 Angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP Transaksi Elektronik) yang menyatakan:

> "Data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasikan secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melakui Sistem Elektronik dan/atau nonelektronik."

Pasal 26 ayat (1) UU ITE menyatakan:

> "Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

Penjelasan Pasal 26 ayat (1) UU ITE menyatakan:

> "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:
>
> d. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
> e. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
> f. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

Dalam RUU Perlindungan Data Pribadi yang masih belum diundangkan, dapat dilihat definisi dari Data Pribadi yaitu dalam Pasal 1 angka 1 bahwa "Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik."

Kegiatan peretasan (selanjutnya disebut hacking) dalam UU ITE walaupun tidak disebutkan secara langsung, dapat masuk dalam definisi yang tertulis dalam Pasal 30 ayat (3) UU ITE, yang menyatakan "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan". Selain pasal tersebut, ada juga Pasal 32 UU ITE yang menyatakan:

1. "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh public dengan keutuhan data yang tidak sebagaimana mestinya."

Pelanggaran atas pasal-pasal tersebut di atas dikenakan jerat hukum sebagaimana disebut dalam Pasal 48 UU ITE sebagai berikut:

1. "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar.
2. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp3 miliar.
3. Setiap Orang yang rnemenuhi unsur sebagaimana dimaksud dalarn Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp5 miliar."

Peraturan mengenai Data Pribadi lainnya dapat ditemukan dalam berbagai peraturan perundang-undangan di Indonesia seperti dalam Pasal 31 ayat (1) Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013, "Pelaku Usaha Jasa Keuangan dilarang dengan cara apapun, memberikan data dan/atau informasi mengenai Konsumennya kepada pihak ketiga." Pasal 57 Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan menentukan bahwa "setiap orang berhak atas kerahasiaan informasi kesehatan pribadinya yang telah diberikan atau dikumpulkan oleh penyedia layanan kesehatan." Namun, berbagai peraturan perundang-undangan ini tidak mengatur perlindungan data pribadi secara spesifik dan hanya terbatas pada sektor-sektor ini, sehingga memungkinkan pihak yang menyalahgunakan atau mencuri data tidak dihukum.

I.6 Pertanggungjawaban Sistematika

Tesis ini terdiri dari 4 (empat) bab dan masing-masing bab terbagi dalam beberapa sub bab. Adapun keempat bab tersebut sebagai berikut:

BAB I Pendahuluan. Bab ini merupakan awal penulisan tesis yang terdiri dari latar belakang dengan mengemukakan kasus pencurian data 91 juta pengguna Tokopedia pada 20 Maret 2020 yang dikaitkan dengan peraturan perundang-undangan yang berlaku tentang perlindungan data pribadi. Selanjutnya bab ini menegaskan mengenai rumusan masalah, tujuan penelitian, dan metode penelitian yang menggunakan yuridis normatif dan diakhiri dengan pertanggungjawaban sistematika.

BAB II Data Pribadi Dan Pengguna Data Pribadi. Bab ini terdiri dari 3 sub bab. Bab II.1 Hakekat dan Pengertian Data Pribadi Menurut UU ITE. Bab ini mengemukakan pengertian data pribadi dan manfaat data pribadi dalam era Industri 4.0. Bab II.2 Pertanggungjawaban Hukum Terhadap Pengguna Data Pribadi. Bab ini mengemukakan pertanggungjawaban hukum terhadap pengguna Data Pribadi menurut UU ITE. Bab II.3 berisi tentang Kasus Pencurian Data Pribadi Pengguna Aplikasi Tokopedia. Diawali dengan kasusnya dan diakhiri dengan analisa pertanggungjawabannya karena dalam pencurian data pribadi ini pasti pihak pemilik Data Pribadi dirugikan materiil maupun imateriil.

BAB III Bentuk Pertanggungjawaban Perusahaan Sebagai Pengelola Data Perusahaan. Bab III terbagi dalam 2 (dua) sub bab. Bab III.1 berisi tentang Pengertian dan Hakekat Pengelola dan Penyimpan Data Pribadi. Bab ini mengemukakan siapakah yang dimaksud dengan pengelola data dan penyimpan data pribadi menurut UU ITE serta kelalaian yang terjadi. Bab III.2 Jenis Pertanggungjawaban Perusahaan Atas Kerugian Akibat Security Breach. Bab ini mengupas bentuk atau jenis pertanggungjawaban perusahaan apabila terjadi kerugian pada pemilik data pribadi apabila terjadi *security breach* dari aspek hukum perdata maupun aspek hukum pidana dan administrasi.

BAB IV Kesimpulan. Bab ini terdiri dari kesimpulan dan saran. Kesimpulan merupakan jawaban singkat atas analisa rumusan masalah sebagaimana dikemukakan pada bab 2 dan bab 3 di atas. Sedangkan saran berupa rekomendasi atau preskripsi dalam bentuk input/masukan terkait untuk menangani dan/atau menyelesaikan permasalahan yang sama atau serupa di masa yang akan datang.